UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,117	07/24/2003	Peter Dam Neilsen	884A.0016.U1(US)	3924

29683 7590 11/06/2006

HARRINGTON & SMITH, LLP
4 RESEARCH DRIVE
SHELTON, CT 06484-6212

EXAMINER	
VAUTROT, DENNIS L	

ART UNIT	PAPER NUMBER
2167	

DATE MAILED: 11/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/627,117	NEILSEN ET AL.	
	Examiner	Art Unit	
	Dennis L. Vautrot	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/24/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Receipt is acknowledged of the amendment to add Patrick Frey as an inventor, dated April 28, 2004. The record has been updated to reflect this change.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 3 November 2003 has been received and entered into the record. Since the IDS complies with the provisions of MPEP § 609, the references cited therein have been considered by the examiner. See attached form PTO-1449.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 19 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 19 recites a method for controlling access rights to data stored in a hand portable device. In order for the method to represent tangible subject matter, it must be useful, concrete and tangible. The method is both useful and concrete, however, it is not tangible. The end result of the method is that the data assemblage is automatically password protected. This does not produce a tangible result.

5. Claims 47, 49, and 51 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Because it was not defined otherwise in the spec, examiner interprets "record carrier" as being a carrier wave transmission medium. According to Annex IV of the "Interim Guidelines for Examination of Patent Applications for Subject Matter Eligibility" that was signed on October 26, 2005 and posted at http://www.uspto.gov/web/offices/pac/dapp/ogsheet.html, a carrier wave is considered to be nonstatutory subject matter because it does not fall into any of the four statutory classes of invention.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 19, 20, 23, 24, and 50 are rejected under 35 U.S.C. 102(e) as being anticipated by **Muratov et al.** (US Patent Application Publication 2003/0097596).

8. Regarding claim 19, **Muratov et al.** discloses a method for controlling access rights to data stored in a hand portable device, wherein a data assemblage containing data for display as displayable content, is automatically password protected after the content is first displayed. (See paragraph [0040] and [0041] "It should be noted that the present invention preferably encrypts the selected databases automatically when the PDA is turned off... Further, and for example, any new database or application loaded into the PDA is encrypted by default until deselected...") In this case, automatic protection is provided upon the loading of new data/applications as well as when the PDA is turned off. This is also interpreted to mean the data was displayed upon receipt, and then automatically password protected based on the setting being set to automatic.

9. Regarding claims 20 and 50, **Muratov et al.** discloses a method for controlling access rights to data stored in a hand portable device, comprising: a) storing a plurality of data assemblages in the hand portable device (Further, different types of encryption may be selected for different types of data (e.g., public records and private records). These different types (public and private records) consist of a plurality of data assemblages); b) storing at least one data attribute for each data assemblage (See paragraph [0081] "Private record field – show/hide (mask) options are available to allow for showing, hiding or masking private records in the databases of the PDA); c) changing the data attribute of a first data assemblage from a first type to a second type (See paragraph [0084] "Encryption field – allows for selecting one of four encryption

modes during PDA locking – No (i.e., no encryption at all); All private Records; A Private Records from selected databases; All from list (i.e. all records from selected databases." Here the type can be changed by adjusting the value in the field.); and d) in response to step c), automatically restricting further access to the first data assemblage using a first security mechanism (See paragraph [0042] "Thus in operation, the present invention provides for encrypting any portion of the data within the PDA that is selected." By changing the data attribute, it would be automatically selected, thus protected).

10. Regarding claim 23, **Muratov et al.** additionally discloses "e) changing the data attribute of a second data assemblage from a first type to a second type (See paragraph [0084] "(4) Encryption field – allows for selecting one of four encryption modes during PDA locking: No (i.e. no encryption at all); All Private Records; A Private Records from selected databases; All from list (i.e., all records from selected databases"); and f) in response to step e), automatically restricting further access to the second data assemblage using the first security mechanism. (See paragraph [0044] "Further, different types of encryption may be selected for different types of data (e.g., public records and private records). All data selected for encryption is automatically encrypted when the PDA is locked (e.g., when powered off).") As can be seen here, depending on the value of the data attribute, changing from one type to another can cause the automatic restriction of the data assemblage.

11. Regarding claim 24, **Muratov et al.** additionally discloses user specification of at least the second type of attribute. (See paragraph [0039] "As shown therein, a checkbox is selected to identify particular applications, and specifically the associated data, that is to be protected.") Here, by checking the box, the attribute can be changed by the user from one type to another (i.e. protected to unprotected). This would apply to any of the attribute fields (first, second, or otherwise).

12. Claims 25, 27, 33, 35, and 41 are rejected under 35 U.S.C. 102(e) as being anticipated by **Kobayashi et al.** (US 6,275,825).

13. Regarding claim 25, **Kobayashi et al.** discloses a hand-portable device, for providing controlled access to stored data assemblages, comprising: user input means for user input of a password (See column 4, lines 1-3); a memory for storing a first data assemblage and a second data assemblage (See column 3, lines 49-52); access means for enabling a user to access the first data assemblage and the second data assemblage (See column 3, lines 1-7); and access control means arranged to detect access to the first data assemblage and automatically restrict subsequent access to the first data assemblage using a first security mechanism involving the password and arranged to detect access to the second data assemblage and automatically restrict subsequent access to the second data assemblage using the first security mechanism involving the password (See column 5, lines 27-33 "The user access right management file UMF is automatically generated on the basis of the contents of the employee

information file (DB), the item access right automatic generation definition file FGF, the record access right automatic generation file, the login management information file LMF, and the login management information linking definition file LLF." and column 6, lines 46-51 "Access right information of each item is input and designated by describing a predetermined symbol in correspondence with each user group at each intersection of the matrix consisting of the row and column captions. In this case, when item access is permitted or allowed, a circle is written in the intersection area..."). The LMF is part of the security mechanism involving the password, which automatically restricts subsequent access as described in the claim. Here, the user is allowed access until the file is accessed and the level of protection is set. Upon setting the level of protection needed, the file is automatically protected.

14. Regarding claim 27, **Kobayashi et al.** discloses the access control means is arranged to restrict subsequent access to the first data assemblage after detecting a first access to the first data assemblage and is arranged to restrict subsequent access to the second data assemblage after detecting a first access to the second data assemblage. (See column 5, lines 27-33 "The user access right management file UMF is automatically generated on the basis of the contents of the employee information file (DB), the item access right automatic generation definition file FGF, the record access right automatic generation file, the login management information file LMF, and the login management information linking definition file LLF." and column 6, lines 46-51 "Access right information of each item is input and designated by describing a predetermined

symbol in correspondence with each user group at each intersection of the matrix consisting of the row and column captions. In this case, when item access is permitted or allowed, a circle is written in the intersection area..."). The LMF is part of the security mechanism involving the password, which automatically restricts subsequent access as described in the claim. Either the data is automatically set because the default is set to automatically restrict access after the first access, or the user sets the particular data type to be protected during the first, or subsequent, access.

15. Regarding claim 33, **Kobayashi et al.** discloses a hand-portable device, for providing controlled access to stored data assemblages, comprising: user input means for user input of a password (See column 4, lines 1-3); a memory for storing data (See column 3, lines 49-52); access means for enabling a user to access the data (See column 3, lines 1-7); and access control means arranged to detect access to the data and automatically restrict subsequent access to the data using a first security mechanism involving the password (See column 5, lines 27-33 "The user access right management file UMF is automatically generated on the basis of the contents of the employee information file (DB), the item access right automatic generation definition file FGF, the record access right automatic generation file, the login management information file LMF, and the login management information linking definition file LLF." and column 6, lines 46-51 "Access right information of each item is input and designated by describing a predetermined symbol in correspondence with each user group at each intersection of the matrix consisting of the row and column captions. In

this case, when item access is permitted or allowed, a circle is written in the intersection area..."). The LMF is part of the security mechanism involving the password, which automatically restricts subsequent access as described in the claim.

16. Regarding claim 35, **Kobayashi et al.** discloses the access control means is arranged to restrict subsequent access to the data after detecting a first access to the data. (See column 5, lines 27-33 "The user access right management file UMF is automatically generated on the basis of the contents of the employee information file (DB), the item access right automatic generation definition file FGF, the record access right automatic generation file, the login management information file LMF, and the login management information linking definition file LLF." and column 6, lines 46-51 "Access right information of each item is input and designated by describing a predetermined symbol in correspondence with each user group at each intersection of the matrix consisting of the row and column captions. In this case, when item access is permitted or allowed, a circle is written in the intersection area..."). The LMF is part of the security mechanism involving the password, which restricts subsequent access as described in the claim. After the first access, the device can either be set to automatically restrict any access, or base the restriction upon data type or username as specified during the access.

17. Regarding claim 41, **Kobayashi et al.** discloses a hand-portable device, for providing controlled access to stored data assemblages, comprising: user input means

for user input of a password (See column 4, lines 1-3); a memory for storing a plurality of data assemblages and a plurality of associated respective attributes (See column 3, lines 49-52); access means for enabling a user to access a stored data assemblage (See column 3, lines 1-7); and access control means arranged to automatically restrict subsequent access to a first data assemblage using a first security mechanism, after the data attribute of the first data assemblage changes from a first type to a second type. (See column 5, lines 27-33 "The user access right management file UMF is automatically generated on the basis of the contents of the employee information file (DB), the item access right automatic generation definition file FGF, the record access right automatic generation file, the login management information file LMF, and the login management information linking definition file LLF." and column 6, lines 46-51 "Access right information of each item is input and designated by describing a predetermined symbol in correspondence with each user group at each intersection of the matrix consisting of the row and column captions. In this case, when item access is permitted or allowed, a circle is written in the intersection area..."). The LMF is part of the security mechanism involving the password, which automatically restricts subsequent access as described in the claim.

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 1, 3, 4, 9, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cragun** (US 6,785,680) in view of **Kobayashi et al.** (US 6,275,825).

20. Regarding claim 1 and 46, **Cragun** teaches a method for controlling access rights to data stored in a hand portable device, comprising: a) storing a plurality of data assemblages in the hand portable device; b) accessing a first data assemblage (See column 7 lines 45-52 "Portable digital device receives and stores the information, acting on it in the conventional manner appropriately to the type of event as if the event had been entered by the user"); **Cragun** fails to teach c) in response to step b), automatically restricting subsequent access to the first data assemblage using a first security mechanism; d) accessing a second data assemblage; and e) in response to step d), automatically restricting subsequent access to the second data assemblage using the first security mechanism. However, **Kobayashi et al.** teaches c) in response to step b), automatically restricting subsequent access to the first data assemblage using a first security mechanism; d) accessing a second data assemblage; and e) in response to step d), automatically restricting subsequent access to the second data assemblage using the first security mechanism (See column 5, lines 27-33 "The user access right management file UMF is automatically generated on the basis of the contents of the employee information file (DB), the item access right automatic generation definition file FGF, the record access right automatic generation file, the login management information file LMF, and the login management information linking

definition file LLF." and column 6, lines 46-51 "Access right information of each item is input and designated by describing a predetermined symbol in correspondence with each user group at each intersection of the matrix consisting of the row and column captions. In this case, when item access is permitted or allowed, a circle is written in the intersection area...") It would have been obvious to one with ordinary skill in the art to combine the access control method of **Kobayashi et al.** with the method as disclosed in **Cragun** because of the need to control access to the data in the portable device. By providing user lookup table, in this example, the data is only permitted to be accessed by a user with proper credentials. If there was no access code assigned for the data, access would also be blocked. It is for this reason that one of ordinary skill in the art would have been motivated to, in response to step b), automatically restrict subsequent access to the first data assemblage using a first security mechanism; d) access a second data assemblage; and e) in response to step d), automatically restrict subsequent access to the second data assemblage using the first security mechanism.

21. Regarding claim 3, **Cragun** additionally teaches before step a), receiving the first data assemblage at the hand portable device and before step d), receiving the second data assemblage at the hand portable device. (See column 7, lines 44-48 "The record is then automatically transmitted via transmitter to portable digital device 303. Portable digital device 303 receives and stores the information, acting on it in the conventional manner appropriately to the type of event as if the event had been entered by the

user.") Here, the data is received by a transceiver. A second data assemblage would be received in the same manner.

22. Regarding claim 4, **Cragun** additionally teaches the access at step b) is a first access to the first data assemblage by the hand portable device and wherein the access at step e) is a first access to the second data assemblage by the hand portable device. (See column 7, lines 49-52 "...the portable digital device will remind the client by beeping, displaying, or other appropriate means at the established time; if the event is an appointment, the data will be entered in the client's appointment calendar so that the client may view it on demand; etc.") The first time the appointment data is being accessed here is by the hand portable device, rather than having to have been entered in by hand.

23. Regarding claim 9, **Cragun** additionally teaches the first data assemblage and/or the second data assemblage is/are created in the device. (See column 2, lines 11-15 "Conventionally, calendar events are entered into a PDA device in one of two ways. The events may be entered manually, or the events may be downloaded from a user's desktop...") Here, the calendar events entered manually, would be an example of a data assemblage being created in the device. This is just once example of a type of data that is manually entered in (i.e. "created") on the device. Because not all data is received from other sources, it would have been obvious to one with ordinary skill in the art to provide for a method of data to be created in the device itself.

24. Claims 2, and 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cragun** in view of **Kobayashi et al.** as applied to claim 1 above, and further in view of **Muratov et al.** (US Patent Application Publication 2003/0097596).

25. Regarding claim 2, **Cragun** and **Kobayashi et al**. teach a method substantially as claimed. **Cragun** and **Kobayashi et al**. fail to teach subsequent to step c), requesting entry of a first password to enable access to the first data assemblage and subsequent to step e), requesting entry of the first password to enable access to the second data assemblage. However, **Muratov et al.** teaches subsequent to step c), requesting entry of a first password to enable access to the first data assemblage and subsequent to step e), requesting entry of the first password to enable access to the second data assemblage. (See paragraph [0008] "The method further may include requiring entry of a password to access the data within the portable electronic device, determining whether the entered password is the valid password, and allowing access to the data if the valid password is entered" and paragraph [0035] "It should be noted that all access to the data through the PDA is locked until the correct password is entered.") It would have been obvious to one with ordinary skill in the art to combine the usage of a password with the access control device. Passwords are commonly known to be one method of access control for data. It is for this reason that one of ordinary skill in the art would have been motivated to include subsequent to step c), requesting entry of a first password to enable access to the first data assemblage and subsequent to

step e), requesting entry of the first password to enable access to the second data assemblage.

26. Regarding claim 5, **Cragun** and **Kobayashi et al**. teach a method substantially as claimed. **Cragun** and **Kobayashi et al**. fail to teach discriminating the type of a data assemblage, wherein the automatic restriction of further access at step c) is enabled only for a first data assemblage of a defined type or types and the automatic restriction of further access at step e) is enabled only for a second data assemblage of the defined type or types. However, **Muratov et al.** teaches discriminating the type of a data assemblage, wherein the automatic restriction of further access at step c) is enabled only for a first data assemblage of a defined type or types and the automatic restriction of further access at step e) is enabled only for a second data assemblage of the defined type or types. (See paragraphs [0039 and 0041] "For example, on a PDA operating on Palm OS®, all record databases (e.g., .pdb files) are encrypted by default, and all resource databases (e.g., .prc files) are not encrypted. Further, and for example, any new database or application loaded into the PDA is encrypted by default until deselected...") Here, depending on the type of file, it would automatically be determined to either be protected information or not protected. This repeats for subsequent data assemblages as well. One with ordinary skill in the art would have seen the usefulness of automatically protecting certain types of files and would have combined the automatic restriction with the access control method. It is for this reason that one of ordinary skill in the art would have been motivated to discriminate the type of a data assemblage,

wherein the automatic restriction of further access at step c) is enabled only for a first data assemblage of a defined type or types and the automatic restriction of further access at step e) is enabled only for a second data assemblage of the defined type or types.

27. Regarding claim 6, **Cragun** and **Kobayashi et al**. teach a method substantially as claimed. **Cragun** and **Kobayashi et al**. fail to teach user specification of the defined type(s) for which automatic restriction of further access is enabled. However, **Muratov et al.** teaches user specification of the defined types for which automatic restriction of further access is enabled. (See paragraph [0039] "As shown therein, a checkbox is selected to identify the particular applications and specifically the associated data, that is to be protected.") It would have been obvious to one with ordinary skill in the art to allow the user to specify which types of data should be automatically restricted in combination with the access control method as described. It is for this reason that one of ordinary skill in the art would have been motivated to allow user specification of the defined types for which automatic restriction of further access is enabled.

28. Regarding claim 7, **Cragun** and **Kobayashi et al**. teach a method substantially as claimed. **Cragun** and **Kobayashi et al**. fail to teach user specification of a password for use in the first security mechanism. However, **Muratov et al.** teaches user specification of a password for use in the first security mechanism. (See paragraph [0082] "Password field – shows password status (i.e., assigned or unassigned), and

provides for assigning (i.e., entering) a new password, changing the current password, or deleting the existing password.") It would have been obvious to one with ordinary skill in the art to combine an access control method having a password with the ability to have the user specify the password as those passwords are often the most easily remembered, among other reasons. It is for this reason that one of ordinary skill in the art would have been motivated to allow user specification of a password for use in the first security mechanism.

29. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Cragun** in view of **Kobayashi et al.** as applied to claim 1 above, and further in view of **Hurst et al.** (US Patent Application Publication 2003/0224823). **Cragun** and **Kobayashi et al.** teach a method substantially as claimed. **Cragun** and **Kobayashi et al.** fail to teach the first data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks and wherein the second data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks. However, **Hurst et al.** teaches the first data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks and wherein the second data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks. (See paragraph [0057] "The activation address and any accompanying data may be transmitted using any known

wireless transmission protocol or messaging service, such as WAP, SMS, EMS, MMS, GPRS, etc.") One with ordinary skill in the art would recognize that many different types of data can be stored on a portable device and would have included the different types as possible data types. The idea that there would be more than one data assemblage is obvious in that the device is designed to hold multiple types of data. It is for this reason that one of ordinary skill in the art would have been motivated to include the first data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks and wherein the second data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks.

30. Claims 10, 12, 13, 18, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cragun** (US 6,785,680) in view of **Kobayashi et al.** (US 6,275,825).

31. Regarding claims 10 and 48, **Cragun** teaches a method for controlling access rights to data stored in a hand portable device, comprising: a) storing data in the hand portable device; b) accessing the stored data (See column 7 lines 45-52 "Portable digital device receives and stores the information, acting on it in the conventional manner appropriately to the type of event as if the event had been entered by the user"). Here "acting on it" is considered accessing the data. **Cragun** fails to teach c) in response to step b), automatically restricting further access to the data. However, **Kobayashi et al.** teaches c) in response to step b), automatically restricting further

access to the data (See column 5, lines 27-33 "The user access right management file UMF is automatically generated on the basis of the contents of the employee information file (DB), the item access right automatic generation definition file FGF, the record access right automatic generation file, the login management information file LMF, and the login management information linking definition file LLF." and column 6, lines 46-51 "Access right information of each item is input and designated by describing a predetermined symbol in correspondence with each user group at each intersection of the matrix consisting of the row and column captions. In this case, when item access is permitted or allowed, a circle is written in the intersection area...") It would have been obvious to one with ordinary skill in the art to combine the access control method of **Kobayashi et al.** with the method as disclosed in **Cragun** because of the need to control access to the data in the portable device. By providing user lookup table, in this example, the data is only permitted to be accessed by a user with proper credentials. If there was no access code assigned for the data, access would also be blocked. It is for this reason that one of ordinary skill in the art would have been motivated to, in response to step b), automatically restrict further access to the data.

32. Regarding claim 12, **Cragun** additionally teaches before step a), receiving at least a portion of the data at the hand portable device. (See column 7, lines 44-48 "The record is then automatically transmitted via transmitter to portable digital device 303. Portable digital device 303 receives and stores the information, acting on it in the

conventional manner appropriately to the type of event as if the event had been entered by the user.") Here, the data is received by a transceiver.

33. Regarding claim 13, **Cragun** additionally teaches the access at step b) is a first access to the data by the hand portable device (See column 7, lines 49-52 "...the portable digital device will remind the client by beeping, displaying, or other appropriate means at the established time; if the event is an appointment, the data will be entered in the client's appointment calendar so that the client may view it on demand; etc.") The first time the appointment data is being accessed here is by the portable device, rather than having been entered in by hand or accessed previously.

34. Regarding claim 18, **Cragun** additionally teaches the data is created in the device. (See column 2, lines 11-15 "Conventionally, calendar events are entered into a PDA device in one of two ways. The events may be entered manually, or the events may be downloaded from a user's desktop...") Here, the calendar events entered manually, would be an example of a data assemblage being created in the device. This is just once example of a type of data that is manually entered in (i.e. "created") on the device. Because not all data is received from other sources, it would have been obvious to one with ordinary skill in the art to provide for a method of data to be created in the device itself.

35. Claims 11, and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Cragun** in view of **Kobayashi et al.** as applied to claim 10 above, and further in view of **Muratov et al.** (US Patent Application Publication 2003/0097596).

36. Regarding claim 11, **Cragun** and **Kobayashi et al**. teach a method substantially as claimed. **Cragun** and **Kobayashi et al**. fail to teach subsequent to step c), requesting entry of a password to enable access to data. However, **Muratov et al.** teaches subsequent to step c), requesting entry of a password to enable access to data. (See paragraph [0008] "The method further may include requiring entry of a password to access the data within the portable electronic device, determining whether the entered password is the valid password, and allowing access to the data if the valid password is entered" and paragraph [0035] "It should be noted that all access to the data through the PDA is locked until the correct password is entered.") It would have been obvious to one with ordinary skill in the art to combine the usage of a password with the access control device. Passwords are commonly known to be one method of access control for data. It is for this reason that one of ordinary skill in the art would have been motivated to include subsequent to step c), requesting entry of a password to enable access to data.

37. Regarding claim 14, **Cragun** and **Kobayashi et al**. teach a method substantially as claimed. **Cragun** and **Kobayashi et al**. fail to teach discriminating the type of a data, wherein the automatic restriction of further access at step c) is enabled only for

data of a defined type or types. However, **Muratov et al.** teaches discriminating the type of a data assemblage, wherein the automatic restriction of further access at step c) is enabled only for data of a defined type or types. (See paragraphs [0039 and 0041] "For example, on a PDA operating on Palm OS®, all record databases (e.g., .pdb files) are encrypted by default, and all resource databases (e.g., .prc files) are not encrypted. Further, and for example, any new database or application loaded into the PDA is encrypted by default until deselected...") Here, depending on the type of file, it would automatically be determined to either be protected information or not protected. One with ordinary skill in the art would have seen the usefulness of automatically protecting certain types of files and would have combined the automatic restriction with the access control method. It is for this reason that one of ordinary skill in the art would have been motivated to discriminate the type of a data assemblage, wherein the automatic restriction of further access at step c) is enabled only for data assemblage of a defined type or types.

38. Regarding claim 15, **Cragun** and **Kobayashi et al**. teach a method substantially as claimed. **Cragun** and **Kobayashi et al**. fail to teach user specification of the defined type(s) for which automatic restriction of further access is enabled. However, **Muratov et al.** teaches user specification of the defined type(s) for which automatic restriction of further access is enabled. (See paragraph [0039] "As shown therein, a checkbox is selected to identify the particular applications and specifically the associated data, that is to be protected.") It would have been obvious to one with ordinary skill in the art to

allow the user to specify which types of data should be automatically restricted in combination with the access control method as described. It is for this reason that one of ordinary skill in the art would have been motivated to allow user specification of the defined types for which automatic restriction of further access is enabled.

39. Regarding claim 16, **Cragun** and **Kobayashi et al**. teach a method substantially as claimed. **Cragun** and **Kobayashi et al**. fail to teach user specification of a password for a first security mechanism used to restrict further access to the data. However, **Muratov et al.** teaches user specification of a password for a first security mechanism used to restrict the further access to the data. (See paragraph [0082] "Password field – shows password status (i.e., assigned or unassigned), and provides for assigning (i.e., entering) a new password, changing the current password, or deleting the existing password.") It would have been obvious to one with ordinary skill in the art to combine an access control method having a password with the ability to have the user specify the password as those passwords are often the most easily remembered, among other reasons. It is for this reason that one of ordinary skill in the art would have been motivated to allow user specification of a password for a first security mechanism used to restrict the further access to the data.

40. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Cragun** in view of **Kobayashi et al.** as applied to claim 10 above, and further in view of **Hurst et al.** (US Patent Application Publication 2003/0224823). **Cragun** and **Kobayashi et al**.

teach a method substantially as claimed. **Cragun** and **Kobayashi et al**. fail to teach the data defines one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks. However, **Hurst et al.** teaches the a data defines one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks. (See paragraph [0057] "The activation address and any accompanying data may be transmitted using any known wireless transmission protocol or messaging service, such as WAP, SMS, EMS, MMS, GPRS, etc.") One with ordinary skill in the art would recognize that many different types of data can be stored on a portable device and would have included the different types as possible data types. It is for this reason that one of ordinary skill in the art would have been motivated to include the data defines one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks.

41. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Muratov et al.** (US Patent Application Publication 2003/0097596) as applied to claim 20, further in view of **Constant et al.** (US Patent Application Publication 2003/0154446).

42. Regarding claim 21, **Muratov et al.** teaches a method for controlling access rights to data stored in a hand portable device substantially as claimed. **Muratov et al.** fails to teach the first type of data attribute indicates that its associated data assemblage

has not yet been accessed using the device and the second type of data attribute indicates that the associated data assemblage has been accessed using the device. **Constant et al.**, however teaches the first type of data attribute indicates that its associated data assemblage has not yet been accessed using the device and the second type of data attribute indicates that the associated data assemblage has been accessed using the device. (See paragraph [0031] "Message database stores message data corresponding to messages created by users. In one embodiment, each message is stored in a table including the following fields for each message: 1) a unique message identifier...and 8) a flag indicating whether the message has been viewed.") Here, the flag is indicative of whether the message has been accessed or not. One with ordinary skill in the art would have recognized the advantage of including an attribute indicator for determining whether data has been accessed in order to alert the user that new data exists on the device that they may not be aware of. It is for this reason that one of ordinary skill in the art would have been motivated to have the first type of data attribute indicate that its associated data assemblage has not yet been accessed using the device and the second type of data attribute indicate that the associated data assemblage has been accessed using the device.

43. Regarding claim 22, **Muratov et al.** teaches a method for controlling access rights to data stored in a hand portable device substantially as claimed. **Muratov et al.** fails to teach the first type of data attribute indicates that its associated data assemblage has been received and is available for access and the second type of data attribute

indicates that the associated data assemblage was not accessed when received. **Constant et al.**, however teaches the first type of data attribute indicates that its associated data assemblage has been received and is available for access and the second type of data attribute indicates that the associated data assemblage was not accessed when received. (See paragraph [0031] and [0049]"Message database stores message data corresponding to messages created by users. In one embodiment, each message is stored in a table including the following fields for each message: 1) a unique message identifier; 2) a recipient identifier...and 8) a flag indicating whether the message has been viewed... When a user opts to check received messages, graphical message server retrieves all message entries where the user is identified in the recipient field and displays a message retrieval interface including the list of retrieved messages.") The data attribute here that displays whether the message is received and available for access is the recipient identifier – if the recipient's name is in the field, then it is available for access to the user of the device. The second data attribute is found in the "flag indicating whether the message has been viewed" (i.e. accessed). One with ordinary skill in the art would have included the first data attribute in order to facilitate the receipt of the proper data and the second data attribute in order to allow the device to differentiate between new messages and messages that have been accessed. It is for this reason that one of ordinary skill in the art would have been motivated to have the first type of data attribute indicate that its associated data assemblage has been received and is available for access and the second type of data attribute indicate that the associated data assemblage was not accessed when received.

44. Claims 26, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kobayashi et al.** (US 6,275,825) as applied to claim 25 above, and further in view of **Cragun** (US 6,78,680).

45. Regarding claim 26, **Kobayashi et al.** teaches a device substantially as claimed. **Kobayashi et al.** fails to teach a transceiver means for receiving a data assemblage at the hand portable device. However, **Cragun** teaches a transceiver means for receiving a data assemblage at the hand portable device. (See column 7, lines 44-48 "The record is then automatically transmitted via transmitter to portable digital device 303.") Here, the data is received by a transceiver. One with ordinary skill in the art would have recognized that a transceiver is an effective way to receive data onto a portable device. It is for this reason that one of ordinary skill in the art would have been motivated to include a transceiver means for receiving a data assemblage at the hand portable device.

46. Regarding claim 32, **Kobayashi et al.** teaches a device substantially as claimed. **Kobayashi et al.** fails to teach the first data assemblage and/or the second data assemblage is/are created in the device. However, **Cragun** teaches the first data assemblage and/or the second data assemblage is/are created in the device. (See column 2, lines 11-15 "Conventionally, calendar events are entered into a PDA device in one of two ways. The events may be entered manually, or the events may be

downloaded from a user's desktop...") Here, the calendar events entered manually, would be an example of a data assemblage being created in the device. This is just once example of a type of data that is manually entered in (i.e. "created") on the device. Because not all data is received from other sources, it would have been obvious to one with ordinary skill in the art to provide for a method of data to be created in the device itself. It is for this reason that one of ordinary skill in the art would have been motivated to include the first data assemblage and/or the second data assemblage is/are created in the device.

47. Claims 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kobayashi et al.** as applied to claim 25 above, and further in view of **Muratov et al.** (US Patent Application Publication 2003/0097596).

48. Regarding claim 28, **Kobayashi et al.** teaches a device substantially as claimed. Kobayashi et al. fails to teach the access control means discriminates the type of a data assemblage, and automatically restricts subsequent access to that data assemblage using a first security mechanism, if the data assemblage is of a defined type or types. However **Muratov et al.**, teaches the access control means discriminates the type of a data assemblage, and automatically restricts subsequent access to that data assemblage using a first security mechanism, if the data assemblage is of a defined type or types. (See paragraphs [0039 and 0041] "For example, on a PDA operating on Palm OS®, all record databases (e.g., .pdb files) are encrypted by default, and all

resource databases (e.g., .prc files) are not encrypted. Further, and for example, any new database or application loaded into the PDA is encrypted by default until deselected...") Here, depending on the type of file, it would automatically be determined to either be protected information or not protected. One with ordinary skill in the art would have seen the usefulness of automatically protecting certain types of files and would have combined the automatic restriction with the access control method. It is for this reason that one of ordinary skill in the art would have been motivated to have the access control means discriminate the type of a data assemblage, and automatically restricts subsequent access to that data assemblage using a first security mechanism, if the data assemblage is of a defined type or types.

49. Regarding claim 29, **Kobayashi et al.** teaches a device substantially as claimed. Kobayashi et al. fails to teach the user input means is operable to enable a user to specify the defined type(s). However, **Muratov et al.** teaches the user input means is operable to enable a user to specify the defined type(s). (See paragraph [0039] "As shown therein, a checkbox is selected to identify the particular applications and specifically the associated data, that is to be protected.") It would have been obvious to one with ordinary skill in the art to allow the user to specify the defined types in combination with the device as described in order for the proper classification of the data as either protected or not protected. It is for this reason that one of ordinary skill in the art would have been motivated to have the user input means operable to enable a user to specify the defined type(s).

50. Regarding claim 30, **Kobayashi et al.** teaches a device substantially as claimed. Kobayashi et al. fails to teach the user input means is operable to enable a user to specify the password. However, **Muratov et al.** teaches the user input means is operable to enable a user to specify the password. (See paragraph [0082] "Password field – shows password status (i.e., assigned or unassigned), and provides for assigning (i.e., entering) a new password, changing the current password, or deleting the existing password.") It would have been obvious to one with ordinary skill in the art to combine a device having a password with the ability to have the user specify the password as those passwords are often the most easily remembered, among other reasons. It is for this reason that one of ordinary skill in the art would have been motivated to have the user input means operable to enable a user to specify the password.

51. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Kobayashi et al.** as applied to claim 25 above, and further in view of **Hurst et al.** (US Patent Application Publication 2003/0224823). **Kobayashi et al**. teaches a device substantially as claimed. **Kobayashi et al**. fails to teach the first data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks and wherein the second data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks. However, **Hurst et al.** teaches the first data assemblage is one of: a SMS message, a MMS message, an

instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks and wherein the second data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks. (See paragraph [0057] "The activation address and any accompanying data may be transmitted using any known wireless transmission protocol or messaging service, such as WAP, SMS, EMS, MMS, GPRS, etc.") One with ordinary skill in the art would recognize that many different types of data can be stored on a portable device and would have included the different types as possible data types. The idea that there would be more than one data assemblage is obvious in that the device is designed to hold multiple types of data. It is for this reason that one of ordinary skill in the art would have been motivated to include the first data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks and wherein the second data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks.

52. Claims 34 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kobayashi et al.** (US 6,275,825) as applied to claim 33 above, and further in view of **Cragun** (US 6,78,680).

53. Regarding claim 34, **Kobayashi et al.** teaches a device substantially as claimed. **Kobayashi et al.** fails to teach a transceiver means for receiving the data at the hand

portable device. However, **Cragun** teaches a transceiver means for receiving the data at the hand portable device. (See column 7, lines 44-48 "The record is then automatically transmitted via transmitter to portable digital device 303.") Here, the data is received by a transceiver. One with ordinary skill in the art would have recognized that a transceiver is an effective way to receive data onto a portable device. It is for this reason that one of ordinary skill in the art would have been motivated to include a transceiver means for receiving the data at the hand portable device.

54. Regarding claim 40, **Kobayashi et al.** teaches a device substantially as claimed. **Kobayashi et al.** fails to teach the data are created in the device. However, **Cragun** teaches the data are created in the device. (See column 2, lines 11-15 "Conventionally, calendar events are entered into a PDA device in one of two ways. The events may be entered manually, or the events may be downloaded from a user's desktop...") Here, the calendar events entered manually, would be an example of data being created in the device. This is just once example of a type of data that is manually entered in (i.e. "created") on the device. Because not all data is received from other sources, it would have been obvious to one with ordinary skill in the art to provide for a method of data to be created in the device itself. It is for this reason that one of ordinary skill in the art would have been motivated to include the data are created in the device.

55. Claims 36-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kobayashi et al.** as applied to claim 33 above, and further in view of **Muratov et al.** (US Patent Application Publication 2003/0097596).

56. Regarding claim 36, **Kobayashi et al.** teaches a device substantially as claimed. **Kobayashi et al.** fails to teach the access control means discriminates the type of data, and automatically restricts subsequent access to data using the first security mechanism, if the data is of a defined type or types. However **Muratov et al.**, teaches the access control means discriminates the type of data, and automatically restricts subsequent access to data using the first security mechanism, if the data is of a defined type or types. (See paragraphs [0039 and 0041] "For example, on a PDA operating on Palm OS®, all record databases (e.g., .pdb files) are encrypted by default, and all resource databases (e.g., .prc files) are not encrypted. Further, and for example, any new database or application loaded into the PDA is encrypted by default until deselected...") Here, depending on the type of file, it would automatically be determined to either be protected information or not protected. One with ordinary skill in the art would have seen the usefulness of automatically protecting certain types of files and would have combined the automatic restriction with the access control method. It is for this reason that one of ordinary skill in the art would have been motivated to have the access control means discriminate the type of data, and automatically restrict subsequent access to data using the first security mechanism, if the data is of a defined type or types.

57. Regarding claim 37, **Kobayashi et al.** teaches a device substantially as claimed. **Kobayashi et al**. fails to teach the user input means is operable to enable a user to specify the defined type(s). However, **Muratov et al.** teaches the user input means is operable to enable a user to specify the defined type(s). (See paragraph [0039] "As shown therein, a checkbox is selected to identify the particular applications and specifically the associated data, that is to be protected.") It would have been obvious to one with ordinary skill in the art to allow the user to specify the defined types in combination with the device as described in order for the proper classification of the data as either protected or not protected. It is for this reason that one of ordinary skill in the art would have been motivated to have the user input means operable to enable a user to specify the defined type(s).

58. Regarding claim 38, **Kobayashi et al.** teaches a device substantially as claimed. **Kobayashi et al.** fails to teach the user input means is operable to enable a user to specify the password. However, **Muratov et al.** teaches the user input means is operable to enable a user to specify the password. (See paragraph [0082] "Password field – shows password status (i.e., assigned or unassigned), and provides for assigning (i.e., entering) a new password, changing the current password, or deleting the existing password.") It would have been obvious to one with ordinary skill in the art to combine a device having a password with the ability to have the user specify the password as those passwords are often the most easily remembered, among other reasons. It is for

this reason that one of ordinary skill in the art would have been motivated to have the user input means operable to enable a user to specify the password.

59. Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Kobayashi et al.** as applied to claim 33 above, and further in view of **Hurst et al.** (US Patent Application Publication 2003/0224823). **Kobayashi et al**. teaches a device substantially as claimed. **Kobayashi et al**. fails to teach the data defines one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks. However, **Hurst et al.** teaches the data defines one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks. (See paragraph [0057] "The activation address and any accompanying data may be transmitted using any known wireless transmission protocol or messaging service, such as WAP, SMS, EMS, MMS, GPRS, etc.") One with ordinary skill in the art would recognize that many different types of data can be stored on a portable device and would have included the different types as possible data types. It is for this reason that one of ordinary skill in the art would have been motivated to include the data defines one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks.

60. Claims 42 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Muratov et al.** (US Patent Application Publication 2003/0097596) as applied to

claim 41, further in view of **Constant et al.** (US Patent Application Publication 2003/0154446).

61. Regarding claim 42, **Muratov et al.** teaches a hand portable device substantially as claimed. **Muratov et al.** fails to teach the first type of attribute indicates that its associated data assemblage has not yet been accessed using the device and the second type of attribute indicates that the associated data assemblage has been accessed using the device. **Constant et al.**, however teaches the first type of attribute indicates that its associated data assemblage has not yet been accessed using the device and the second type of attribute indicates that the associated data assemblage has been accessed using the device. (See paragraph [0031] "Message database stores message data corresponding to messages created by users. In one embodiment, each message is stored in a table including the following fields for each message: 1) a unique message identifier...and 8) a flag indicating whether the message has been viewed.") Here, the flag is indicative of whether the message has been accessed or not. One with ordinary skill in the art would have recognized the advantage of including an attribute indicator for determining whether data has been accessed in order to alert the user that new data exists on the device that they may not be aware of. It is for this reason that one of ordinary skill in the art would have been motivated to have the first type of attribute indicate that its associated data assemblage has not yet been accessed using the device and the second type of attribute indicate that the associated data assemblage has been accessed using the device.

62. Regarding claim 43, **Muratov et al.** teaches a hand portable device substantially as claimed. **Muratov et al.** fails to teach the first type of attribute indicates that its associated data assemblage has been received and is available for access and the second type of attribute indicates that the associated data assemblage was not accessed when received. **Constant et al.**, however teaches the first type of attribute indicates that its associated data assemblage has been received and is available for access and the second type of attribute indicates that the associated data assemblage was not accessed when received. (See paragraph [0031] and [0049]"Message database stores message data corresponding to messages created by users. In one embodiment, each message is stored in a table including the following fields for each message: 1) a unique message identifier; 2) a recipient identifier...and 8) a flag indicating whether the message has been viewed... When a user opts to check received messages, graphical message server retrieves all message entries where the user is identified in the recipient field and displays a message retrieval interface including the list of retrieved messages.") The attribute here that displays whether the message is received and available for access is the recipient identifier – if the recipient's name is in the field, then it is available for access to the user of the device. The second attribute is found in the "flag indicating whether the message has been viewed" (i.e. accessed). One with ordinary skill in the art would have included the first attribute in order to facilitate the receipt of the proper data and the second attribute in order to allow the device to differentiate between new messages and messages that have been

accessed. It is for this reason that one of ordinary skill in the art would have been motivated to have the first type of attribute indicate that its associated data assemblage has been received and is available for access and the second type of attribute indicate that the associated data assemblage was not accessed when received.

63. Claims 44 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kobayashi et al.** as applied to claim 41 above, and further in view of **Muratov et al.** (US Patent Application Publication 2003/0097596).

64. Regarding claim 44, **Kobayashi et al.** teaches a hand portable device substantially as claimed. **Kobayashi et al.** fails to teach the access control means is arranged to automatically restrict subsequent access to a second data assemblage using a first security mechanism, when the data attribute of the second data assemblage changes from a first type to a second type. **Muratov et al.**, however teaches the access control means is arranged to automatically restrict subsequent access to a second data assemblage using a first security mechanism, when the data attribute of the second data assemblage changes from a first type to a second type. (See paragraph [0084] "(4) Encryption field – allows for selecting one of four encryption modes during PDA locking: No (i.e. no encryption at all); All Private Records; A Private Records from selected databases; All from list (i.e., all records from selected databases" and See paragraph [0044] "Further, different types of encryption may be selected for different types of data (e.g., public records and private records). All data selected for

encryption is automatically encrypted when the PDA is locked (e.g., when powered off).") As can be seen here, depending on the value of the data attribute, changing from one type to another can cause the automatic restriction of the data assemblage. It would have been obvious to one with ordinary skill in the art to aid in the proper security of the data. It is for this reason that one of ordinary skill in the art would have been motivated to have the access control means arranged to automatically restrict subsequent access to a second data assemblage using a first security mechanism, when the data attribute of the second data assemblage changes from a first type to a second type.

65. Regarding claim 45, **Kobayashi et al.** teaches a hand portable device substantially as claimed. **Kobayashi et al.** fails to teach the user input means enable user specification of at least the second type of attribute. However, **Muratov et al.** teaches the user input means enable user specification of at least the second type of attribute. (See paragraph [0039] "As shown therein, a checkbox is selected to identify particular applications, and specifically the associated data, that is to be protected.") Here, by checking the box, the attribute (second or otherwise), can be changed by the user from one type to another (i.e. protected to unprotected). It would have been obvious to one with ordinary skill in the art to allow user specification of the type of attributes in order to facilitate the proper categorization of the data. Some would need to be protected, while it would not be crucial for other data. It is for this reason that one

of ordinary skill in the art would have been motivated to include user input means that enable user specification of at least the second type of attribute.

Conclusion

66. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Adams et al. (US 6,487,646) teaches a method for restricting access to data on a storage device.

Bertina et al. (US 6,145,739) teaches encryption and data restriction methods for various intelligent devices.

Kulack et al. (US Patent Application Publication 2004/0143750) teaches security enhancements for PDAs mostly using tokens, but also mentions passwords alone as an alternative.

Tani (US Patent Application Publication 2004/0092247) teaches an auto dial-lock method.

Non Patent Related Documents

Author: Hongyuan Chen and T.V.L.N Sivakumar; Title: Access Control for Future Mobile Devices; Date: 2005; Publisher: IEEE Communications Society; WCNC 2005.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dennis L. Vautrot whose telephone number is 571-272-2184. The examiner can normally be reached on Monday-Friday 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Breene can be reached on 571-272-4107. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

dlv

Luke S. Wassum
Primary Examiner
Art Unit 2167

John E. Breene
SUPERVISORY PATENT EXAMINER